Modern SecOps
dans l'écosystème Microsoft

2026

Comment les entreprises suisses peuvent renforcer durablement leur cyberrésilience grâce aux fonctions de sécurité existantes





01

Des fonctions de sécurité à la **résilience opérationnelle**

Les entreprises suisses qui utilisent déjà les solutions de sécurité Microsoft font face à un dilemme : malgré les nombreuses fonctionnalités disponibles, un écart subsiste avec une cyberrésilience réellement efficace.

Cet écart apparaît lorsque les fonctions de sécurité restent isolées, que les signaux ne sont pas centralisés, que les équipes IT évaluent manuellement les alertes et que les données ne sont pas clairement classifiées. La complexité augmente alors même que les exigences réglementaires, les cyberrisques et les attentes de la direction se renforcent.

Modern SecOps comble cet écart. L'approche réunit protection, détection, réponse, contrôle des données et amélioration continue dans un modèle opérationnel clair. Microsoft fournit la plateforme intégrée. Axians Somnitec la rend opérationnelle pour les entreprises suisses grâce à l'architecture, la gouvernance, la mise en œuvre, l'exploitation et l'optimisation continue.

Les solutions de sécurité Microsoft deviennent ainsi plus qu'un ensemble d'outils. Les entreprises gagnent en visibilité sur leurs risques, priorisent les mesures selon leur impact, exploitent mieux leurs licences et déchargent leurs équipes internes. Elles réagissent plus rapidement aux menaces et améliorent leur posture de sécurité de manière mesurable.

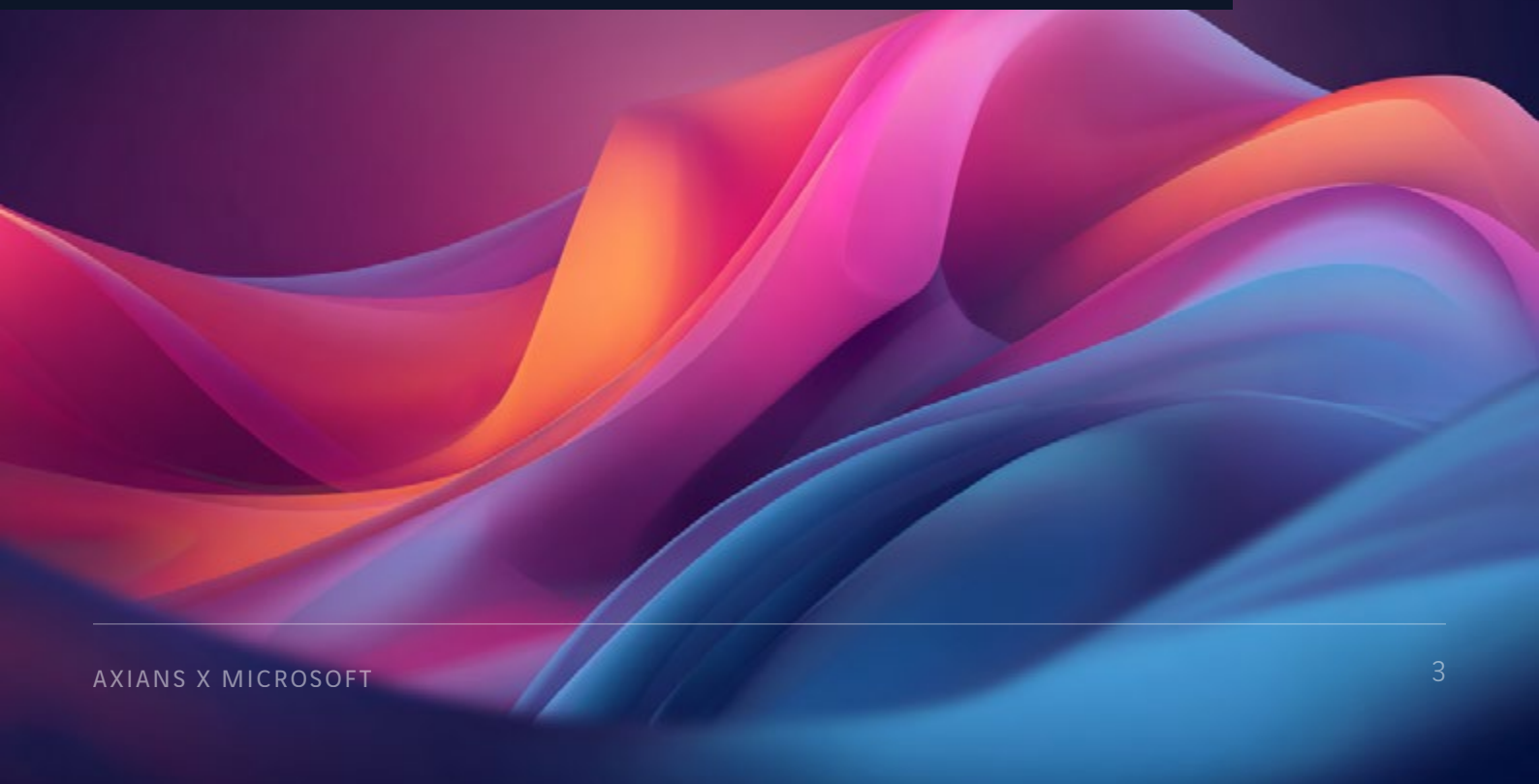
Ce guide montre comment faire évoluer votre environnement Microsoft Security vers un modèle opérationnel de sécurité, afin de faire de la cybersécurité un levier de stabilité, de conformité et de confiance.

02

Complexité de la sécurité malgré l'investissement dans Microsoft

Dans les entreprises suisses, le niveau de sécurité reste souvent en deçà du potentiel des solutions Microsoft acquises.

Il manque un modèle opérationnel intégré. Les fonctions de sécurité sont exploitées en parallèle plutôt qu'ensemble. Ainsi, malgré le recours à un fournisseur éprouvé et à de nombreuses fonctionnalités, la complexité augmente et le niveau de sécurité diminue.



Les causes les plus fréquentes

01

Des licences disponibles, mais sous-utilisées.

Les entreprises paient souvent pour des fonctions qu'elles n'utilisent que partiellement, notamment Microsoft 365 E5, Defender, Entra, Purview ou Sentinel. Sans feuille de route claire, difficile de savoir quelles capacités sont disponibles et comment les exploiter.

02

Les outils de sécurité restent cloisonnés.

Même dans l'écosystème Microsoft, la sécurité ne fonctionne pas automatiquement de manière intégrée. Signaux, politiques, rôles et processus doivent être coordonnés pour offrir une vision claire.

03

Les alertes génèrent des efforts plutôt que de la clarté.

Les équipes de sécurité reçoivent de nombreuses alertes, sans toujours disposer de priorités claires. Sans corrélation ni processus de réponse défini, chaque alerte doit être analysée individuellement.

04

Les données restent difficiles à maîtriser.

Les entreprises ne savent pas toujours où se trouvent leurs données sensibles, qui y a accès et comment elles sont protégées. Avec l'essor de l'IA, de Copilot et du cloud, cet enjeu devient critique.

05

Les évaluations restent ponctuelles.

Un Secure Score ou un audit ne montre qu'un état à un instant donné. La cyberrésilience exige de mesurer, prioriser et réduire les risques en continu.

Ce que cela signifie pour les entreprises suisses

En Suisse, ces défis s'inscrivent dans un environnement particulièrement exigeant. Les entreprises doivent garantir disponibilité, protection des données, conformité et confiance, souvent sur plusieurs sites, régions linguistiques et dans différents contextes réglementaires. Parallèlement, les directions, clients et partenaires attendent des réponses solides face aux cyberrisques.



03

Modern SecOps : La sécurité comme état opérationnel



Face à cette évolution, les entreprises adoptent souvent de nouveaux outils, de nouvelles politiques ou des projets ponctuels. Mais la technologie seule ne réduit pas la complexité. Au contraire, sans intégration claire, la charge opérationnelle continue d'augmenter.

Modern SecOps adopte donc une autre approche.

L'accent n'est pas mis sur des produits de sécurité individuels, mais sur des opérations de sécurité intégrées. L'objectif est d'identifier les risques plus tôt, d'évaluer les menaces plus rapidement et d'améliorer en continu les mesures de sécurité, à travers les identités, les terminaux, les environnements cloud, les applications et les données. La sécurité n'est ainsi plus considérée comme un ensemble de mesures isolées, mais comme un processus continu et orchestré de manière centralisée.

Ce que Modern SecOps change

Modern SecOps réunit prévention, détection, réponse et gouvernance dans un modèle intégré. Les signaux de sécurité sont centralisés, les risques priorisés et les équipes bénéficient de plus de contexte et de moins de contraintes opérationnelles.

Le focus se déplace ainsi :

» des outils isolés

» de la corrélation manuelle

» de la gestion réactive des incidents

Pour aller vers :

» une visibilité continue

» une priorisation automatisée

» une réponse plus rapide

» une amélioration mesurable de la posture de sécurité

Pour les entreprises, cela signifie avant tout : **plus de maîtrise.**

Les responsables de la sécurité disposent d'une vision plus claire des risques, des chemins d'attaque et des vulnérabilités. La pression sur les équipes internes diminue grâce à des processus standardisés, des signaux centralisés et l'automatisation des tâches récurrentes.

Les **quatre piliers** de Modern SecOps

Un modèle de sécurité moderne repose sur quatre capacités essentielles :

Optimiser le SOC en continu

Les opérations de sécurité évoluent en permanence. Les entreprises améliorent continuellement leurs règles de détection, leurs processus de réponse et leurs politiques de sécurité, plutôt que seulement après un audit ou un incident.

Rendre les surfaces d'attaque visibles

Les plateformes de sécurité modernes analysent les liens entre identités, appareils, ressources cloud et autorisations. Les risques peuvent ainsi être détectés plus tôt et mieux priorisés.

Détecter les menaces dans leur ensemble

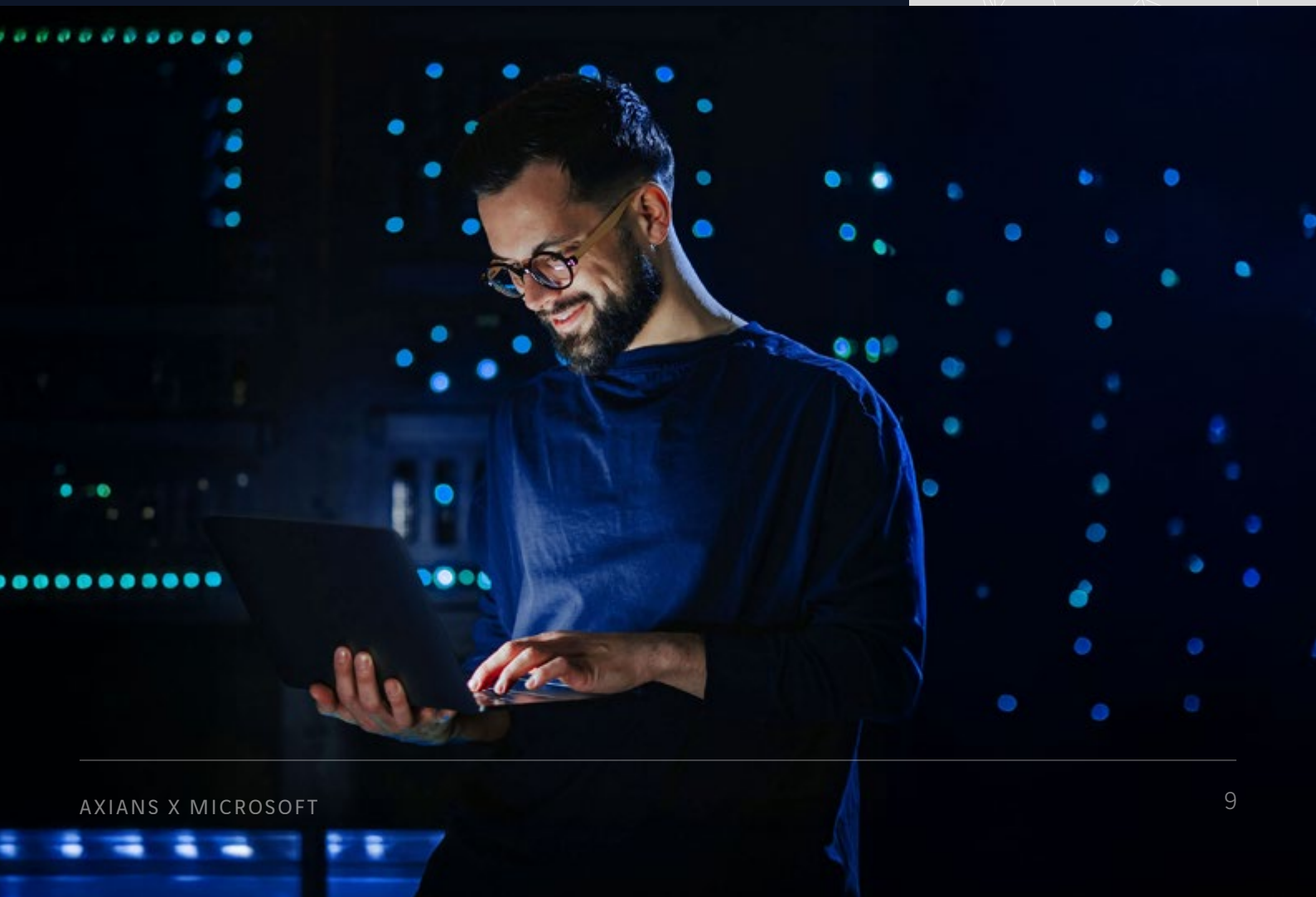
Les attaques se limitent rarement à un seul point. Modern SecOps regroupe les signaux de différents domaines afin d'offrir une vision globale de l'environnement.

Réagir plus vite et plus intelligemment

L'automatisation et l'IA aident les équipes de sécurité à analyser les incidents, à prioriser les mesures et à accélérer les processus de réponse.

La différence essentielle

Modern SecOps ne remplace pas une stratégie de sécurité existante. L'approche réunit les capacités disponibles dans un modèle opérationnel global. Pour de nombreuses entreprises suisses, c'est précisément la prochaine étape : ne plus seulement utiliser les fonctions de sécurité Microsoft sur le plan technique, mais en faire des opérations de sécurité robustes et pilotées en continu.



La plateforme **Microsoft Unified Security**

04

Une architecture de sécurité doit centraliser les informations plutôt que de les traiter séparément. C'est dans cette logique que Microsoft a conçu ses solutions de sécurité comme une plateforme intégrée.

Les identités, terminaux, e-mails, services cloud, applications et données génèrent en continu des signaux de sécurité. La plateforme Microsoft Unified Security relie ces différents niveaux dans un modèle commun.

Connecter la sécurité à tous les niveaux

Microsoft Defender XDR constitue la base opérationnelle pour la détection et la réponse. La plateforme centralise les signaux de différents domaines afin de créer un contexte de sécurité commun.

Microsoft Sentinel complète ce modèle avec des fonctions centralisées d'analyse et d'automatisation.

Avec **Microsoft Entra** l'identité devient centrale. Les accès, autorisations et contextes utilisateurs sont évalués en continu afin d'identifier les risques et d'appliquer les principes Zero Trust.

Microsoft Purview ajoute la dimension des données. Les entreprises gagnent en visibilité sur leurs informations sensibles, leur utilisation et leur protection.

Security Copilot aide enfin les équipes à analyser plus rapidement les informations, à mieux comprendre les corrélations et à accélérer les processus de réponse.

Des signaux isolés à la maîtrise opérationnelle

La force de cette plateforme réside dans l'orchestration. Une connexion suspecte n'est plus analysée isolément : elle peut être corrélée avec les appareils, les accès aux données, le comportement des utilisateurs ou les activités cloud. Ce contexte renforce l'efficacité des opérations de sécurité.

Les entreprises bénéficient ainsi de :

- Plus de visibilité sur les risques
- Moins de contraintes opérationnelles
- Une priorisation plus rapide
- Des processus de sécurité plus cohérents
- Une meilleure base pour la gouvernance et la conformité

05

La sécurité des données comme base d'une utilisation sûre de l'IA

Avec l'essor de l'IA, le rôle de la cybersécurité évolue. Les entreprises ne protègent plus seulement les appareils, les comptes utilisateurs ou les applications. Les données elles-mêmes deviennent centrales. Les systèmes d'IA utilisent les informations que les entreprises créent, stockent et partagent au quotidien. Plus l'IA s'intègre aux processus de travail, plus une question devient essentielle :

Quelles données un système peut-il consulter, traiter ou partager ?

La sécurité des données devient ainsi un élément central des stratégies de sécurité modernes.



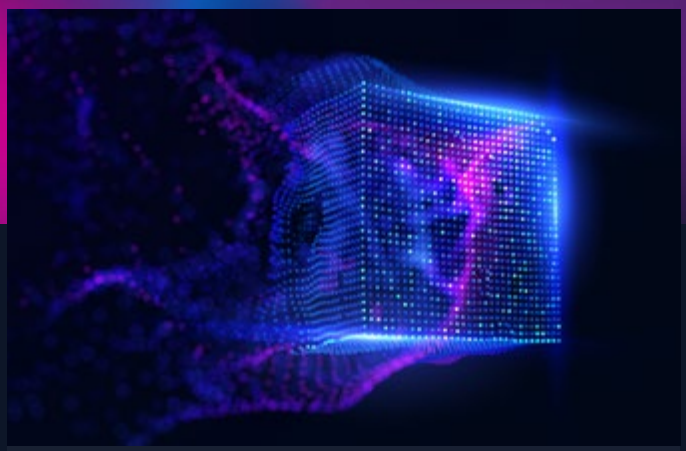


L'IA accroît les exigences de gouvernance et de transparence

Cela crée de nouveaux défis :

- accès trop large aux données sensibles
- autorisations difficiles à contrôler
- données mal classifiées ou non protégées
- perte du contexte de sécurité
- conformité et protection des données plus complexes

L'IA rend ainsi les vulnérabilités existantes plus visibles et souvent plus critiques..



La sécurité des données exige du contexte

La sécurité périmétrique classique ne suffit plus. Les entreprises doivent comprendre :

- où se trouvent les données sensibles
- qui peut y accéder
- comment les informations sont utilisées
- quels risques découlent des partages, des services cloud ou de l'utilisation de l'IA

Microsoft Purview complète l'architecture de sécurité en apportant cette perspective. Les données peuvent être classifiées, des politiques de protection définies et les accès mieux contrôlés.

Microsoft Purview complète l'architecture de sécurité en apportant précisément cette perspective. Les données peuvent être classifiées, des politiques de protection définies et les accès mieux contrôlés.

En Suisse, cette approche revêt une importance particulière. La protection des données, les exigences réglementaires et la gestion responsable des informations jouent un rôle central pour les entreprises, leurs clients et leurs partenaires.

06

De la sécurité ponctuelle à la résilience continue

La protection des données, la gouvernance et la sécurité des données ne peuvent plus être considérées séparément. Elles sont directement liées à la capacité d'une entreprise à résister aux cyberrisques.

C'est pourquoi il ne suffit plus d'évaluer la sécurité ponctuellement. La sécurité se construit en continu. Les risques évoluent, les modes d'attaque s'adaptent et les environnements numériques changent constamment. Les entreprises ont donc besoin d'une approche qui améliore la sécurité en permanence.

Des fonctions telles que Secure Score, Exposure Management ou Attack Path Analysis permettent de :

01 Identifier rapidement les failles de sécurité

02 Prioriser les risques selon leur impact réel

03 Détecter les chemins d'attaque critiques

04 Mesurer les progrès dans le temps

05 Améliorer les mesures de sécurité de manière ciblée

Au lieu de mesures isolées, un cycle continu d'évaluation, de priorisation, de mise en œuvre et d'optimisation se met en place.

De la sécurité ponctuelle à la résilience continue

Il est essentiel de comprendre les interactions entre les risques. Un risque isolé peut sembler mineur jusqu'à ce qu'il se combine à d'autres vulnérabilités.

Un accès oublié, des autorisations trop larges ou des données sensibles non protégées peuvent créer ensemble des chemins d'attaque critiques. Les plateformes de sécurité modernes permettent de rendre ces liens visibles.

Cela change aussi la manière de prioriser la sécurité au quotidien. Les équipes ne se concentrent plus uniquement sur le nombre d'alertes ou de vulnérabilités, mais sur leur impact réel sur les risques de l'entreprise.



07

De la plateforme aux opérations sécurisées avec Axians Somnitec

Même les plateformes les plus performantes ne révèlent pleinement leur valeur que lorsque les entreprises ne se limitent pas à identifier les risques, mais en déduisent des processus, des responsabilités et des mesures clairs.

L'enjeu est donc d'intégrer la sécurité de manière cohérente aux opérations quotidiennes. C'est cette intégration dans les processus, les rôles et les opérations de sécurité qui permet de créer une véritable cyberrésilience.Axians Somnitec aide les entreprises à transformer les fonctions de sécurité Microsoft existantes en un modèle intégré, adapté à leur organisation, à leurs risques et à leur infrastructure IT.

L'objectif est de mettre en place des opérations de sécurité pilotables en continu, avec :

01 une base de sécurité solide

02 l'intégration des composants Microsoft Security clés

03 des processus opérationnels et de réponse clairs

04 l'amélioration continue de la posture de sécurité

05 des opérations standardisées pour alléger les équipes internes

Axians associe ainsi technologie, gouvernance, opérations et amélioration stratégique continue.

Un modèle adapté à la réalité suisse

Pour les entreprises suisses, fiabilité, transparence et gouvernance jouent un rôle central, au-delà de la technologie. La sécurité doit être efficace, mais aussi rester compréhensible et maîtrisable, notamment face à la direction, aux clients, aux partenaires et aux exigences réglementaires.

Axians Somnitec associe pour cela Microsoft Security à une expertise opérationnelle locale, des responsabilités claires et une approche Modern SecOps structurée.

Les différentes fonctions de sécurité deviennent ainsi des opérations de sécurité intégrées, qui réduisent les risques, soulagent les équipes internes et renforcent durablement la cyberrésilience.



08

Où en êtes-vous ? Le chemin vers **Modern SecOps**

L'objectif n'est pas de transformer tout le système de sécurité en une seule fois. Les entreprises font évoluer leur organisation progressivement, selon leur niveau de risque, leurs ressources, les exigences réglementaires et leur environnement IT. Ce modèle présente les étapes typiques vers Modern SecOps.

01

NIVEAU DE MATURITÉ 1

Sécurité basée sur les outils

Les fonctions de sécurité Microsoft sont disponibles, mais restent largement isolées.

Caractéristiques :
- nombreux processus manuels
- forte charge liée aux alertes
- visibilité limitée
- sécurité principalement gérée sur le plan technique

02

NIVEAU DE MATURITÉ 2

Plateforme de sécurité intégrée

Les signaux provenant des identités, appareils, environnements cloud et données sont davantage centralisés.

Caractéristiques :
- meilleure visibilité sur les risques
- premières automatisations
- baselines et politiques de sécurité
- posture de sécurité mesurable

03

NIVEAU DE MATURITÉ 3

Opérations Modern SecOps

La sécurité est intégrée à l'organisation et pilotée en continu.

Caractéristiques :
- processus opérationnels et de réponse définis
- monitoring et reporting continus
- priorisation plus claire
- équipes internes déchargées

04

NIVEAU DE MATURITÉ 4

Organisation de sécurité résiliente

La sécurité évolue vers un modèle opérationnel optimisé en continu.

Caractéristiques :
- analyse proactive des risques
- sécurité des données et gouvernance intégrées
- processus assistés par l'IA
- transparence et maîtrise élevées



Prenez contact dès maintenant

Vous souhaitez savoir où vous en êtes aujourd'hui ? Un Modern SecOps Readiness Assessment avec Axians Somnitec vous montre le potentiel déjà présent dans vos solutions Microsoft Security.

Ensemble, nous identifions les mesures qui auront le plus grand impact sur la sécurité et l'activité, en fonction de vos besoins et de vos ressources. Contactez-nous !